Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

Formulating an Advanced Security Protocol for Internet of Medical Things based on Blockchain and Fog Computing Technologies

Rasha Halim Razzaq[1] , Mishall Al-Zubaidie[1]

[1]Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq

*Corresponding author: Rasha Halim Razzaq

DOI: https://doi.org/10.30880/ijcsm.2024.05.03.046
Received April 2024 ; Accepted June 2024; Available online September 2024

ABSTRACT: The Internet of Medical Things (IoMT) is an evolving field in healthcare that connects medical devices to the Internet to enable efficient data sharing and health information collection. The IoMT aims to improve the quality of healthcare, facilitate diagnosis and treatment, and enhance patient safety. Nonetheless, the IoMT networks are usually exposed to multiple security attacks. Also, recent studies indicate that security protocols contain flaws in protecting patient data. Thus, data must be protected by innovative security protocols. In our work, we propose a Medical Security Protocol (MedSecP) to support security in IoMT. The proposed protocol adopts the Twofish encryption, Naive Bayes (NB), and decision tree (DT) within the private blockchain (PBC) Fog Computing (FC) to build robust security procedures. The Twofish encryption algorithm is used to provide medical information concealment. In our proposed protocol, the type of data is first determined, and accurate and appropriate medical decisions are made based on the collected data using a decision tree algorithm, and then rapid classification of the patient data is done using the Naive Bayes algorithm. Confidential medical data is then encrypted using the Twofish algorithm to ensure the confidentiality of this data and prevent unauthorized access. Finally, this encrypted medical data is stored using blockchain technology. Twofish, NB, and DT are organized to work harmoniously with the PBC. The latter manages and distributes data peer-to-peer in IoMT. We leverage Fog Computing to speed up decision-making without resorting to the remote cloud. We analyzed our protocol in terms of security and performance. Our results indicate that MedSecP provides reliable security against attacks as the protocol demonstrated an average security attack response rate of 97.20%, demonstrating its resistance to external threats by keeping the encrypted medical data, classified and achieving appropriate medical decisions. In terms of performance, MedSecP has demonstrated an average security response time of around 50ms, providing fast and efficient performance. In MedSecP, the highest value for encryption is 0.000015 ms, and decryption is 0.000017 ms when applying the Twofish algorithm which is considered extremely suitable for implementing health systems operations compared to existing encryption algorithms. Consequently, MedSecP provides lightweight operations in support of complex security measures that qualify it to support healthcare institutions.

Keywords: Decision tree (DT); IoMT; MedSecP; Naive Bayes (NB); private blockchain (PBC); Towfish; Fog Computing (FC); Blockchain.

1. INTRODUCTION

The Internet of Things (IoT) has become one of the basic axes in scientific and practical life. One of its important types is the Internet of Medical Things (IoMT). It is considered one of the most powerful, durable, convenient, and available applications due to the rapid technological progress in collecting huge medical data, deep learning, and cloud computing. The IoMT is an integrated ecosystem that contains interconnected medical sensors, computer systems, and clinical systems. It has received great attention in recent years due to major challenges in the quality and efficiency of medical services and healthcare [1]. Moreover, integration of healthcare systems leads to reducing diagnostic and clinical errors and costs, enhancing patient care, reducing the burden on doctors and healthcare workers, and detecting errors that may expose systems to cyberattacks. Networked healthcare systems are often vulnerable to security, privacy, and availability threats from network servers and peripheral devices [2].

The data collected from IoMT medical devices has a significant impact on the accuracy of predictions in terms of quality, importance, and quantity. Furthermore, classifying medical data according to the data that must be included in the medical diagnosis. Additionally, the fog cloud provides an appropriate authentication method, it selects a section of data to verify and at the same time solves the requests made in real time. Thus, one of the benefits of FC is the use of time as it has priority in work [3]. Also, FC provides a decentralized and scalable network that addresses security,

identification, and authentication issues in patient health data. FC is to collect process data into blocks for validation and is similar in operation to blockchain technology [4]. The IoMT system contains homogeneous and heterogeneous parts, it is vulnerable to security attacks most of the time. Therefore, security studies aim to find security solutions or protection protocols to preserve medical data for fear of hacking it and giving wrong data or wrong medical diagnoses that may lead to the death of patients. Cyberattack has a significant impact on the lives of patients in health centers that rely on electronic records, as in Figure 1 [5]. With an average of 12.5 cyberattacks throughout the 24 months, over half of the surveyed health institutions, 56% reported having been the target of one or more cyberattacks utilizing IoMT devices. 53% of the responders (24% total) stated that the intrusions had a negative influence on patient care, and 45% claimed that the intrusions increased death rates.

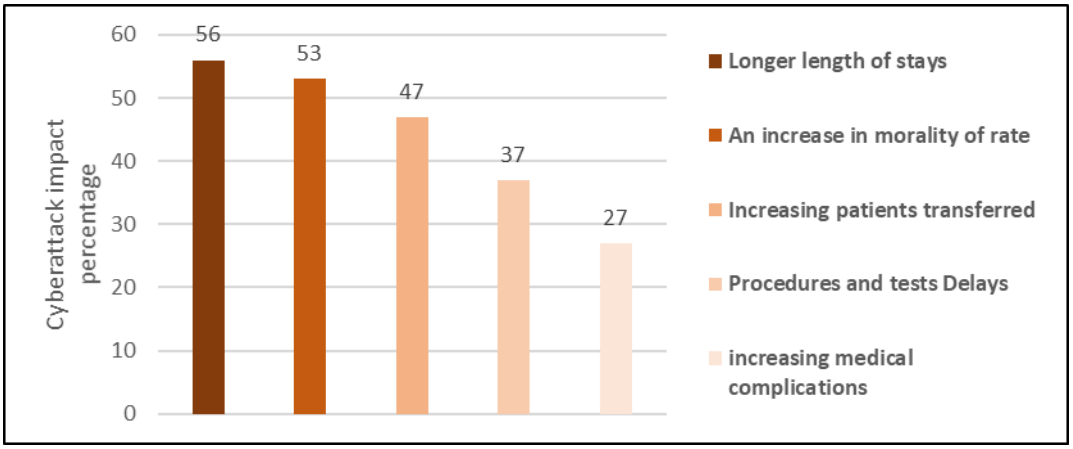

FIGURE 1. Cyberattack effects on e-health

Blockchain is a technology used to store large amounts of data [6]. Blockchain has been positioned as an intriguing innovation that can guarantee the safety of personal information, build a decentralized database, and enhance data interoperability. Also, fog computing has been described as a potential technology that can improve efficiency, decrease latency, and enable low-cost remote monitoring. For IoMT applications, combining fog computing and blockchain technology can potentially solve several issues, including automating smart contracts, data integrity, authenticity, privacy, and ownership, reliability, decentralized data storage, standard interoperability, scalability, and performance. Blockchain and FC technologies are being used to provide an IoMT framework to enhance privacy, and security that reduce delays by attacks in healthcare systems. This is done by using blockchain to reliably secure and record patient data and using FC to reduce delays in data transmission and improve system responsiveness. More clearly, the efficiency and security of medical systems based on online medical objects are improved through the use of FC and blockchain technologies. Our new framework provides convenient healthcare for patients with the ability to effectively monitor them remotely, provide timely healthcare, and reduce potential security risks in IoMT systems [6]. Completed transactions are recorded and stored in a shared block distributed across dynamic blockchain network systems. With the growing IoMT, which may reach 22 billion by 2025 [4], this has led to a significant rise in the number leads to security and privacy concerns as these many devices are unable to protect themselves due to their weak processing and nature. Among the attacks that these devices are exposed to are eclipse, malware, man-in-the-middle, zero-day exploits, and many others. To protect these devices from these attacks, it is necessary to identify algorithms or protocols that meet security and encryption needs. Encryption algorithms can contribute to protecting the anonymity of patient data and diagnoses [7,8]. On the other hand, it is necessary to carefully choose encryption algorithms that balance performance and security, especially in applications that deal with huge patient data [9]. The following are the MedSecP's significant contributions:

- Using PCB and FC technologies, a secure and reliable way to store and transmit patient data can be provided without returning to the remote cloud, protecting them from potential security threats.
- Using the NB and DT algorithms, we were able to improve the accuracy of predicting critical medical diagnoses, contributing to improved patient care and making the right medical decisions.
- Our protocol integrates lightweight Twofish encryption with NB and DT which provides security for diagnostics and decisions. To the best of our knowledge, this contribution is innovative because it is the first time this integration has not been implemented in IoMT.

Below is the arrangement of the paper's contents. Section 1 provides an introduction to the topic. Section 2 provides works related to our research topic. Section 3 describes cyberattacks on the IoMT and blockchain. Section 4 presents our protocol methodology. Section 5 presents performance and security results. The conclusion is presented in Section 6.

2. RELATED IOMT SECURITY RESEARCH

This section briefly presents the set of recent research and its drawbacks related to the topic of IoMT security.

Li et al. [1] addressed the integration of Fri-jam (friendly-jamming) schemes with various communication technologies and recommended the use of Fri-jam schemes as a means of safeguarding patients' private medical data that is gathered by medical sensors against cyberattacks. Additionally, they provided two case studies of IoMT Fri-jam techniques. According to their findings, this approach will lessen the likelihood of cyberattacks without having any impact on legal transmission. However, if performance is low, the primary causes of security non-acceptability in electronic applications are the constraints of medical equipment in terms of compute power, memory capacity, and energy supply. A blockchain was examined by Alam et al. [4] as a possible method for reducing the effects of storage and latency issues when used in combination with FC. They demonstrated how blockchain may address security and privacy issues with FC. They also discussed the problems and constraints of blockchain from the viewpoints of FC and IoMT. They investigated how blockchain solves security issues in fog-enabled IoMT. However, their approach did not address the issue of confidentiality of decision-making and diagnoses. Furthermore, Alalhareth and Hong [10] presented an improved method for feature selection in IoMT termed logistic redundancy coefficient gradual upweighting (LRGU), which assesses candidates independently rather than comparing them to shared traits of the features that have previously been chosen. LRGU calculates the logistic function to determine a feature's redundancy score and to identify variations in cyberattack patterns. The experimental evaluation results show that their LRGU can recognize some important features. However, their IoMT application is sometimes exposed to a variety of cyber threats, such as man-in-the-middle attacks and malware, which can compromise device reliability and patient safety and privacy.

Su et al. [11] proposed a protocol called “blockchain-based signal encryption and data management (TB-SCDM) protocol” using blockchain technology for the purpose of authorization and authentication in wireless vehicular networks. The protocol aims to authenticate the identity of users and protect the confidentiality of information when communicating between different vehicles in the network environment. The protocol also aims to repel various attacks, such as Eclipse attacks, half +1 attacks, and double spending attacks. He et al. [12] in their study proposed a hybrid framework using reinforcement learning and deep learning that detects malware in healthcare devices. Device data is converted into small images and neural network models are trained to detect malware. The best model for use in real-time detection of unknown malware is selected using a reinforcement learning-based agent. The research aims to protect patient data and ensure the safety of healthcare systems from security threats. The research needs to provide more effective solutions to deal with (Zero-day) breaches, which are attacks that exploit security vulnerabilities that are not yet known and for which patches have not been released. Mustafa et al. [13] proposed a powerful method to stumble on and prevent dispensed DoS assaults, wherein they used a fixed of supervised machine mastering algorithms which include Random Forests, Decision Trees, XGBoost, K-Nearest Neighbor, and Support Vector Machine, similar to ensemble gaining knowledge of to enhance detection accuracy. The model development procedure consists of collecting and pre-processing facts, dividing them into check and training sets, selecting prediction fashions, and evaluating their performance. The proposed technique changed into evaluated on a dataset containing 11,423 cases, and confirmed promising effects, with accuracy starting from 92% to a hundred% for the time collection dataset. The consequences of data fusion in IoMT, along with the security issues that come with it and possible solutions, were covered by Ahmed et al. [14] and are not widely covered in previous studies. The quality, amount, and relevance of data gathered by IoMT devices directly affect prediction accuracy. The most efficient method for identifying epileptic seizures in IoMT networks is the epilepsy seizures detector-based Naive Bayes (ESDNB) algorithm, which has an accuracy from 99.53% to 99.99%. It has been demonstrated that blockchain technology and cryptography are viable means of enhancing an IoMT system's security. Since data transmitted over the Internet is susceptible to hacking and unauthorized access, privacy and security concerns are of utmost importance. The problem with their approach is that accurate and rapid classification of massive patient data was not used.

3. CYBERATTACKS ON THE IOMT AND BLOCKCHAIN

Cyberattacks are attacks targeting medical computer networks and systems, as well as devices connected to the Internet, IoT, IoMT, whether medical, healthcare organizations, health centers, etc. The goal of these attacks is unauthorized access, disruption of services, theft of information, tampering with data, or electronic piracy. Therefore, individuals and institutions that use the IoT in general, as well as blockchain technology, must take strong security measures to protect their accurate and sensitive data, as well as enhance the security of their used systems, by regularly updating programs and systems, as well as using high-security protocols and systems [15]. Here we will explain some of the important attacks that the IoMT and blockchain are exposed to:

- Eclipse Attacks: These attacks are a type of security attack that exploits vulnerabilities in the IoT wireless network architecture. This is done by disabling or distorting communication signals between devices connected to a particular network. Attackers exploit wireless eclipse, where the communication signal is temporarily interfered with, allowing them to carry out attacks such as disrupting the connection or tampering with data.
- Malware attacks: These attacks are computer programs that are designed to manipulate computers or networks. These attacks can infect medical IoT devices, cause the theft of sensitive data, disable medical devices, or tamper with devices and data. Examples include ransomware, Trojan horses, Viruses, and spyware.

- Man-in-the-Middle Attacks: These attacks are when an attacker infiltrates a connection between two other devices without the original users knowing. This is done by recording, analyzing, and manipulating traffic between connected devices, allowing an attacker to seize, modify, or make unauthorized use of sensitive information.
- Zero-Day Attacks: Attacks that exploit security vulnerabilities in hardware or software that have not yet been disclosed by the manufacturer or developer. Attackers exploit these new vulnerabilities before they are addressed or a patch is released. This means that targeted devices are particularly vulnerable as there is no prior protection against these attacks.

Finally, cyberattacks are constantly evolving, so consideration must be given to constantly improving and enhancing the security of computer systems and networks through the use of modern technologies and strong encryption algorithms in the proposed frameworks to be useful and important frameworks.

4. PROPOSED PROTOCOL METHODOLOGY

Fog computing is a technology that aims to provide computing, storage, and processing resources at a decentralized level in IoMT networks. It aims to improve the performance and responsiveness of Internet applications that require real-time processing and proximity of computational and storage resources to users (patients and nurses, doctors, etc.) or connected devices. FC relies on distributing tasks and processes among connected devices in an IoMT network, instead of sending all the data and processing to the remote cloud. This reduces lag and improves application responsiveness. The technology associated with FC in our protocol is the PBC. It is a type of decentralized technology that allows data to be stored and exchanged securely and transparently. PBC works by recording and confirming transactions in a series of interconnected blocks. These blocks are protected by hashes and hold information about various transactions, including the time, date, and parties involved. FC and PBC overlap in the context of IoMT integration. In our proposed protocol, we also used NB, Twofish, and DT algorithms for security, transparency, accurate medical data tracking, data matching, and medical decision-making. Overall, FC and PBC collaborate to provide reliable and secure solutions in healthcare. In general, the relationship between FC and PBC is that we use FC to provide resources and local processing for IoMT devices and applications. We use PBC to secure and authenticate medical data and achieve security and transparency. This integration led to MedSecP which has helped us improve the quality of healthcare, and provide continuous and effective patient monitoring without the need for expensive and limited human resources. Figure 2 shows our methodology and flow of work steps.

4.1 Medical Security Protocol

In this paper, we propose the Medical Security Protocol (MedSecP). MedSecP addresses the property and security of healthcare data that has been improved after studying many types of specialized research. Within our proposed protocol, we use more than one algorithm (NB, DT, Twofish, PBC) differently, the purpose of which is to increase the performance and quality of IoMTs. Our proposed MedSecP protocol predicts health diagnoses, quickly makes accurate and appropriate medical decisions and analyzes medical data. It then classifies and encrypts the input data with high precision to preserve its privacy. We will include here large and important details about the operation of the DT, NB, and Twofish algorithms. We will also discuss their importance in classifying data, their level of influence on decision-making, and how these algorithms can support the confidentiality and security of sensitive medical information in our proposed medical protocol.

MedSecP's FC is used to encrypt medical data, protect it from malware, man-in-the-middle attacks, Eclipse, and zero-day exploits, and store and protect it in the PBC. We will briefly examine the impact of these algorithms on the operation of the protocol. The first step in the process is to use DT to determine what type of medical data is being collected, and then make informed judgments based on that data. Next, NB is used to classify medical data based on the output of the decision tree algorithm in order to identify relevant medical data. Confidential medical data is then encrypted to ensure its confidentiality and protection from unwanted access using Twofish technology. Assuming medical data, such as patient personal details, symptoms, diagnosis, and treatment course, we provide several examples of using these algorithms in the protocol. DT is used to analyze this data and provide accurate medical recommendations. For example, NB can be used to classify patients into specific and different categories based on their expected precise medical diagnoses. Important medical data is then encrypted using the Twofish algorithm. For example, patient personal information and sensitive medical diagnoses that need confidentiality protection can be encrypted. The encrypted data is then stored using PBC technology to ensure it is secure and has not been tampered with. These examples illustrate practical applications of the algorithms mentioned in the MedSecP, where Twofish, NB, and DT work in an integrated manner to achieve the confidentiality of medical data and make accurate and appropriate medical decisions.

4.2 MedSecP Work Steps and Data Processing

At the beginning of the protocol, it collects medical data related to healthcare devices connected to the IoMT. Then, it receives the list of readings of these devices as input, processes this data, and stores it in the data processing list (CollectedData). As shown in Algorithm 1, this is considered the first step of our proposed MedSecP protocol. This algorithm demonstrates the data collection mechanism.

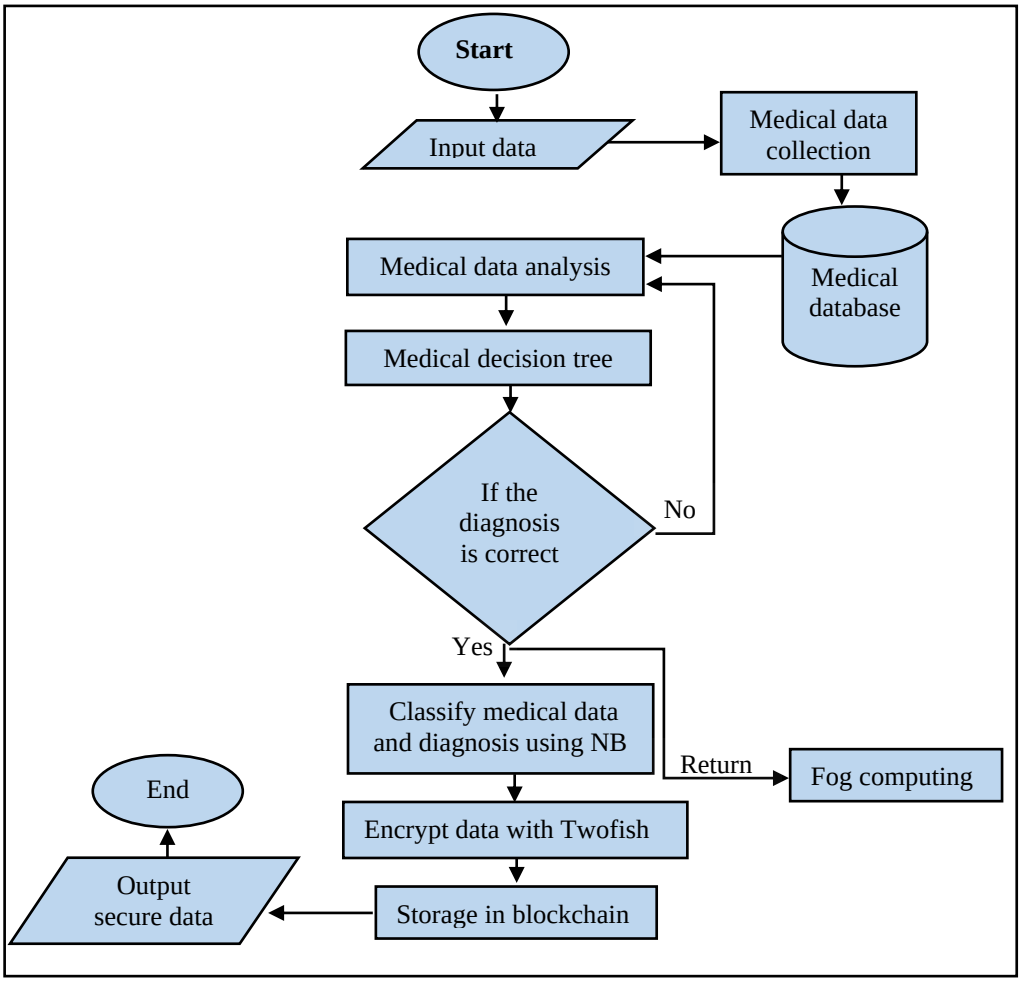

FIGURE 2. Our protocol methodology and work steps

ALGORITHM 1: Collect the first set of data

Input: MedicalIoMTData (a reading list of healthcare-related IoMT devices)
Output: CollectedData (list of processed data)

```
Begin
    Procedure CollectDataFromDevices (MedicalIoMTData):
    CollectedData ← []
    for reading in MedicalIoMTData
        processedData ← ExtractUsefulInformation (reading)
    CollectedData.append (processedData)
End
Return CollectedData
```

In the second step of the MedSecP, we will analyze the data where we receive the processed data set (CollectedData) as input and analyze this data. The AnalyzedData set is updated using the analyst information extracted from each data point in the processed data set. Algorithm 2 describes the data analysis process in MedSecP.

ALGORITHM 2: Data analysis

Input: CollectedData
Output: AnalyzedData
1. Begin
2. AnalyzedData ← []
3. for dataPoint in CollectedData
4. ExtractedInfo ← AnalyzeDataPoint (dataPoint)
5. UpdateAnalyzedData (AnalyzedData, EtractedInfo) ← AnalyzedData
6. End
7. Return AnalyzedData

The third step of our protocol is to build a DT model. We take a list of matched data (MatchedData) and build a DT model. We will use the output results of the analysis algorithm as input to build the DT model. Based on the model created, a medical decision is made. If the model is not empty, it is applied to make the decision. If the model is empty, "Unable to make a decision due to insufficient data" will be returned. Algorithm 3 describes building a DT model in MedSecP.

ALGORITHM 3: Building a DT model

Input: MatchedData
Output: MedicalDecision
1. Begin
2. DecisionTreeModel ← BuildDecisionTreeModel (DataAnalysisResults)
3. MedicalDecision ← []
4. if DecisionTreeModel is not empty
5. MedicalDecision ← ApplyDecisionTreeModel(DecisionTreeModel)
6. Else:
7. MedicalDecision ← "Unable to make a decision due to insufficient data"
8. End
9. Return MedicalDecision

After we designed the decision-making model, the step of training the NB model is the fourth step in our proposed protocol. We take the data set (Dataset Patients_DB) for patients from openneuro website (functional magnetic resonance imaging dataset in the brain) that is available in [16] and the medical decision (MedicalDecision), put them as input, and train a DT model. We set up the probabilities of the categories ($P(C_i)$) and the probabilities of the explanatory variables ($P(Xj|C_i)$) based on the data we provided to the model. We then apply a normalization process to these probabilities. We also generate a random secret key (K) using the NB algorithm, as shown in Algorithm 4.

ALGORITHM 4: NB training

Input: Dataset Patients_DB, MedicalDecision
Output: $P(C_i)$, $P(X_j|C_i)$, and K
1. Begin
2. Initialize: $P(C_i)$ and $P(X_j|C_i)$ for each C_i and X_j provided with zero
3. For each instance in Patients_DB:
4. Update counts for $P(C_i)$ and $P(X_j|C_i)$ using the instance.
5. For each class C_i
6. Normalize $P(C_i)$ and $P(Xj|C_i)$.
7. End
8. Generating random secret key () ← K
9. End
10. Return $P(C_i)$, $P(X_j|C_i)$

The fifth step in MedSecP is using the Twofish encryption algorithm. We take sorted data in the encryption process that includes steps such as key expansion, input whitening, Feistel network, and output whitening. Then, we return the encrypted data (E) as shown in Algorithm 5 (X represents the input data and Y represents the output data). After we obtain the results from the NB outputs and make them inputs to Twofish, we perform the process of whitening the inputs. Then, Twofish divides the input into two parts, applies the 16 rounds to the two parts, and then combines it with the key expanded by XOR. After that, we perform the process of whitening the output to obtain the encrypted data.

ALGORITHM 5: Twofish cipher

Input: Sorted data X from NB.
Output: E
1. Begin
2. Twofish_Key_Expansion(K) ← Key Expansion: K'
3. Input Whitening: X' ← Twofish_Input_Whitening(X)
4. For each block in X'
5. Twofish_Feistel_Network(X', K') ← Perform Feistel Network: Y
6. Output Whitening: E ← Twofish_Output_Whitening(Y)
7. End For
8. End
9. Return E

In our project, we were able to use PBC to store data and distribute them. A PBC is a sequential data structure consisting of a set of blocks linked together by a hash function. At MedSecP, we use PBC to support the management and protection of data from modification.

5. ANALYSIS AND RESULTS

Blockchain and the IoT network in general are exposed to several attacks, and these attacks are attempts to either attack the blockchain network or attack the mining process. Examples include eclipse attacks, phishing attacks, zero-day attacks, and other attacks [15]. In our paper, this section will explain the security analysis of MedSecP and its performance results. Table 1 describes the attack comparison between MedSecP and existing protocols.

5.1 Cyberattacks analysis on Medsecp

1. Eclipse attack: It is an impersonation attack that occurs in peer-to-peer (P2P) environments. An attacker can exploit it to carry out other attacks, such as denial of service attacks, information theft, or data manipulation. This attack is exploited to eliminate a specific victim by controlling the node, or surrounding nodes in a P2P network and directing them to interact with a malicious node controlled by the attacker. Eclipse attacks are dangerous in P2P environments. To protect networks from eclipse attacks, MedSecP uses encryption of data sent and communications over the network. Strong encryption algorithms such as Twofish embedded in our protocol can be used to enhance data security and protect it from unauthorized access, and contribute to protecting and securely storing medical data. Our MedSecP protocol aims to enhance the security and privacy of patient data within IoMT. Therefore, our protocol protects against these attacks.
2. Malware attack: It is one of the most dangerous and threatening attacks on IoMT as it can affect the security of connected healthcare devices and medical data. Malicious software intended to infiltrate systems and steal, alter, or interfere with data is referred to as "malware". Malware attacks can end result from clinical device malfunctions, manipulation, and clinical fact theft. Through the use of software replacement tests, device fitness, and safety exams, records encryption, and anomalous conduct monitoring, our proposed MedSecP protocol gives elevated safety of affected personal information against malware attacks. By enforcing those security features, our proposed MedSecP protocol can help guarantee excessive dependability and keep away from malware assaults to stabilize affected personal information and connected scientific gadgets.
3. Man-in-the-middle (MITM) attack: This type of cyberattack aims to take control of user communications by initiating a hostile attack that targets both the sender and the recipient. The attacker gains access to the sender and recipient's communication chain, allowing them to monitor, record, and alter the sender and recipient's data. In the context of IoMT, unauthorized access to the communication network between linked medical devices—such as portable measurement devices, health monitoring devices, etc.—can result in an MITM. Since our system employs PBC hashing to prohibit alterations and Twofish to disguise patient data, it will be able to fend off MITM attacks on IoMT. This is why the proposed MedSecP security protocol includes mechanisms that will be put in place to repel such attacks. This suggests that our system is capable of precisely and successfully fending off MITM attacks.
4. Zero-day exploit attack: Because the creators were unaware of the vulnerability for zero days prior to an attacker making use of it, the vulnerability is known as "Zero-Day." Since no security update has been released to address this security vulnerability, the goal of this attack is to take advantage of an undiscovered security flaw in electronic devices or applications. In the context of IoMT, a medical device that has outdated software, insufficient security measures, or unidentified vulnerabilities may be subject to a zero-day exploit assault. These vulnerabilities provide the attacker the ability to access the device without authorization and carry out malicious orders, such as stealing confidential information or taking control of the device and altering its functionality. To combat Zero-day exploit attacks, our security protocol can provide security procedures by integrating DT, NB, and Twofish to detect abnormal behavior. However, we should note that complete protection against Zero-Day attacks is impossible, as it relies on vulnerabilities that have not yet been discovered. Therefore, using our encryption protocol, updating

software and hardware, and implementing strong security practices are crucial to enhancing the security of the medical IoMT and reducing its vulnerability to Zero-day exploit attacks.

TABLE 1. Comparison of the MedSecP protocol with similar security protocols

Attack	[4]	[11]	[12]	MedSecP
Anti-Eclipse		Yes		Yes
Anti-Malware	Yes		Yes	Yes
Anti-MITM	Yes			Yes
Anti-Zero-day exploit			Yes	Yes

5.2 MedSecP Performance Results

To authenticate the results, our protocol was implemented in an environment that depends on CPU Intel(R) Core (TM) i5, 8192 MB RAM, Ubuntu Pro 64-bit Operating system, and Java programming language. All our algorithms were implemented 100 times to check MedSecP performance. Figure 3 shows the accuracy of collecting medical data from medical devices and sensors. Medical data sets based on Internet-connected objects can be analyzed in the cloud system, as shown in Figure 4. Moreover, decision trees provide many benefits such as ease of understanding, predictability, and ability to analyze, apply, inspect, and document. In the context of the current research, we used the decision tree algorithm to improve the accuracy of medical diagnosis and reduce security threats in the IoMT, and the results were interesting, as shown in Figure 5. We obtained an increase in the accuracy of medical diagnosis through the use of the NB algorithm. Furthermore, medical data are classified according to the data that should be included in the medical diagnosis, as depicted in Figure 6. The IoMT applications suffer from homogeneous, heterogeneous, clear parts, and thus it is vulnerable to cybersecurity attacks most of the time. Therefore, the MedSecP protocol aimed to find security solutions, preserve patient data, and avoid hacking it or providing false medical data through the use of Twofish encryption, as shown in Figure 7, and Figure 8 shows the encryption and decryption ratios in the Twofish algorithm by executing 1000 responses. From the results in Figures 3-8, it is clear that the proposed procedures (collection data, data analysis, DT, NB, and Twofish) can provide high performance for IoMT applications in e-health institutions.

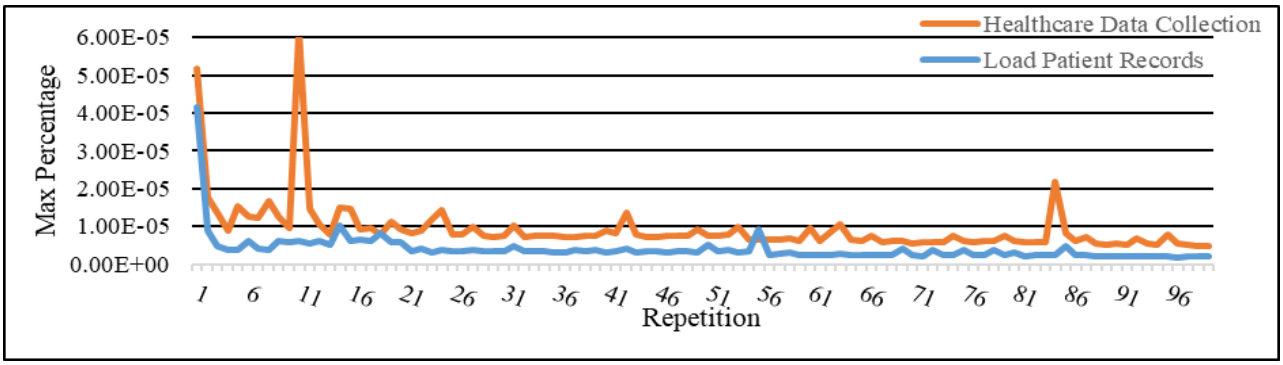

FIGURE 3. Medical data collection

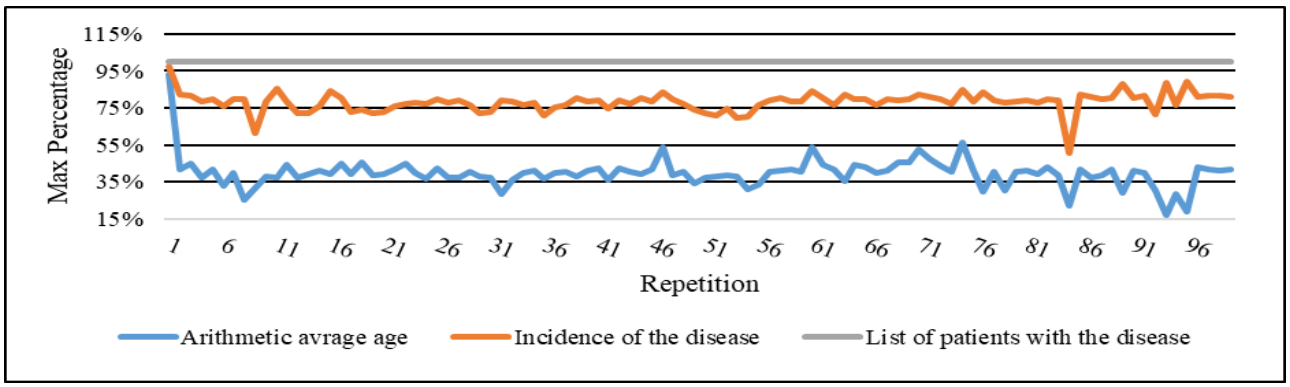

FIGURE 4. Medical data analysis

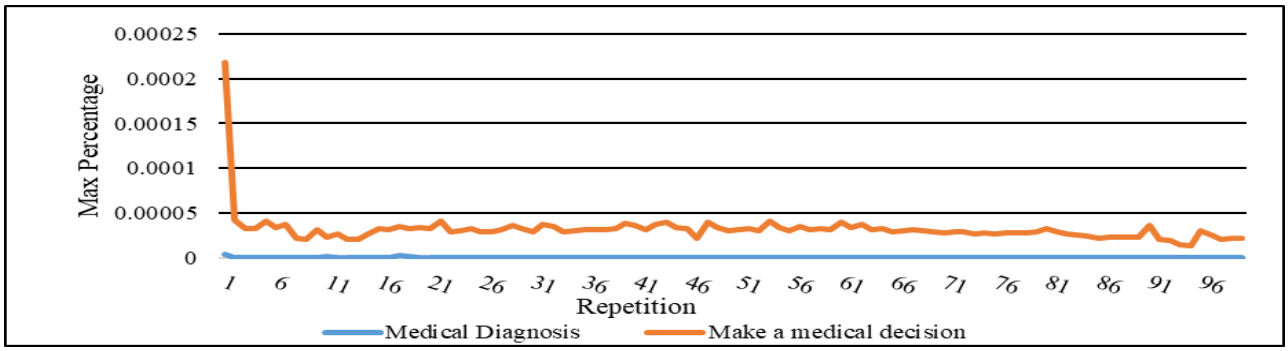

FIGURE 5. DT analysis

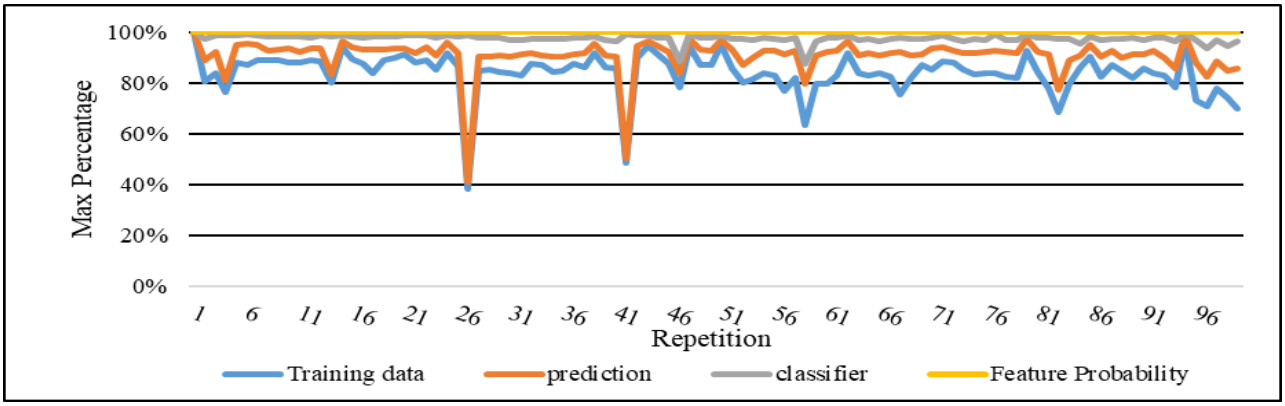

FIGURE 6. NB analysis

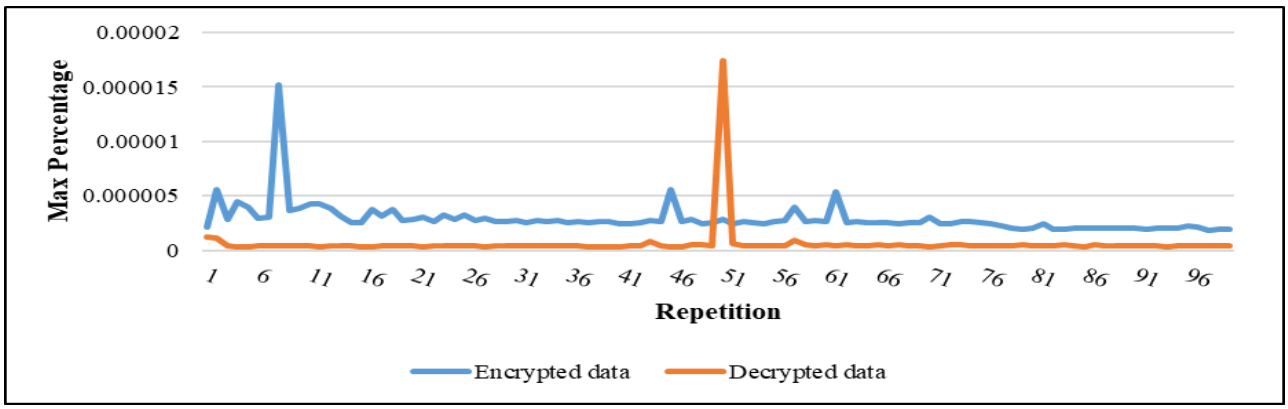

FIGURE 7. Twofish decryption & encryption

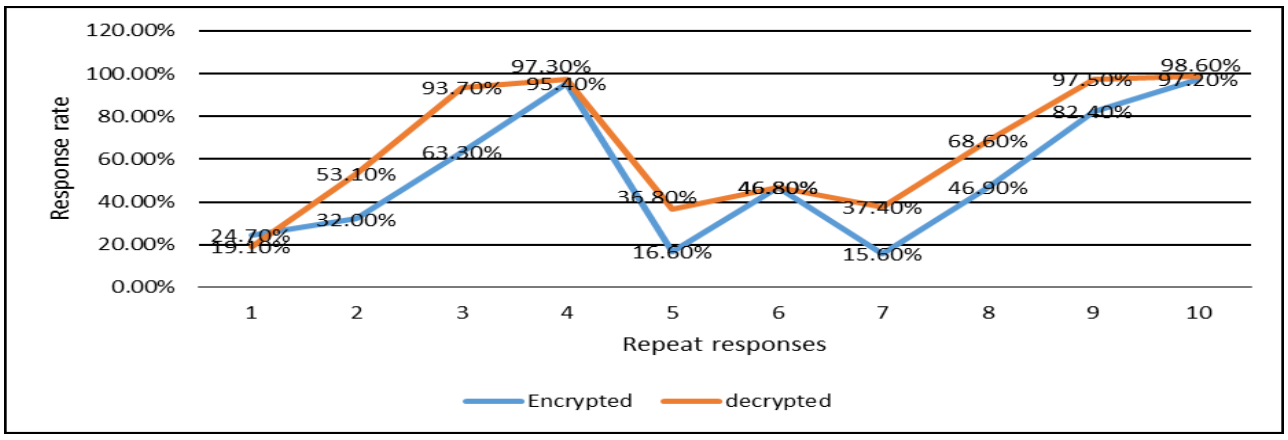

FIGURE 8. Twofish analysis of 1000 implementations

5.3 Evaluation and Metrics

In this study section, we describe the requirements by which the efficacy and overall performance of the algorithms in our advised MedSecP method have been assessed. We also describe how each algorithm satisfies the given goals to what extent and the way to check each algorithm's overall performance. The following metrics are employed:

- Security response Time: It evaluates how long it takes the MedSecP protocol to thwart distinct styles of assaults, which include the malicious ones we studied in this research, and computes how long it takes the protocol to react to safety breaches. It evaluates how properly the protocol has labored to stop these assaults and incursions.
- Diagnostic accuracy: Medical selection-making algorithms and medical information categorization algorithms (NB and DT) are evaluated for correctness and accuracy. The overall performance of the algorithm is likewise evaluated by usage of metrics such as error and detection charges.
- Attack response rate: It evaluates the effectiveness of the protocol and the use of precise overall performance measures, such as detection and reaction rates. This metric shows the extent to which our protocol can fend against security lapses and attacks, as well as the manner in which the proposed protocol handles them.
- Data security: Data security uses various security measures such as the level of protection, security, and strength of encryption, in addition to other measures that work for the purpose of evaluating the success of encryption algorithms in their specific work. Here, it was used to evaluate the effectiveness of the Twofish encryption algorithm in thwarting illegal access to medical data and maintaining its privacy and confidentiality.

To evaluate the performance of our protocol, a comparison between the performances of the MedSecP with the performance of other security protocols. The researchers in [17] noted that Twofish provides better performance in terms of execution time and storage compared to the commonly used advanced encryption standards (AES) algorithm. The average response time was calculated as 50 ms, by dividing the total duration by the number of pre-specified responses. Before that, we determined the average response time for executing our proposed MedSecP protocol and obtained 100 responses (for 1000 executions) within the specified time period. This was verified by setting the maximum number of responses, and it took a total of five seconds to obtain responses. Our MedSecP protocol offers a security response rate of up to 97.20%, which is high and reliable compared with the percentages of different security measures ranging approximately from 62% [18] while in [19] the security response rate was 80%.

6. CONCLUSIONS

In the final part of our study, we will explain the conclusions we obtained to achieve our important and clear goal of enhancing the privacy and security of medical data while reducing the chances of hacking IoMT devices. Our research also aims to improve the identification of security threats to these systems. By using PBC and FC technologies, we were able to provide a reliable and secure way to store and transmit patient data, as well as protect it from expected cyber threats. We designed the MedSecP protocol to support security in IoMT. Our medical encryption protocol is based on the Twofish algorithm to provide reliable protection for medical data. Our protocol also used DT and NB classification and decision-making algorithms to improve patient care, classify patient data, and make valid and accurate medical decisions. Therefore, its performance is lightweight and strong enough to support difficult security measures in Health institutions. The integration of Twofish, PBC, FC, PBC, DT, and NP into the proposed MedSecP framework contributes to protecting medical data from hacking and tampering and reducing the risk of cyberattacks. In Section 4 our results show that MedSecP provides adequate security (malware, eclipse, and Zero-day attacks within the scope of the proposed protocol, and MITM), and also provides high performance in supporting medical data protection in IoMT. For a future framework, we are directing our thoughts to plan to use the Jellyfish algorithm and combine it with NB to remove duplicate entries, reduce overhead, and also support identical data detection. Also, paying attention to updating the encryption keys in Twofish is an important requirement in developing this protocol. The performance of the MedSecP can also be improved by improving the encryption techniques used or improving the efficiency of the decision-making algorithms used such as DT and NB. Other techniques such as deep learning or other artificial intelligence techniques can also be studied to improve the performance of the protocol. Expanding the application of the medical security protocol to other areas of healthcare besides the IoMT could also be explored. For example, the protocol could be used in home health care, telemedical communications, or even in other fields such as clinical pharmacy. We will also explain here potential some of the limitations of the MedSecP. Medical devices have limited resources such as memory, power, and processing. The MedSecP should be compatible with these resources and consume as little resources as possible to maintain device efficiency such as sensors in the IoMT. Additionally, the IoMT environment deals with different types of users, such as the patient, nurse, doctor, pharmacist, etc., which require different levels of authorization when accessing patient data. This limitation needs to be addressed seriously in the future of our MedSecP protocol.

Funding

None

ACKNOWLEDGEMENT

The authors would like to thank the reviewers for providing useful suggestions, allowing for the improved presentation of this paper.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] X. Li, H. N. Dai, Q. Wang, M. Imran, D. Li, and M. A. Imran, (2020). “Securing Internet of medical things with friendly-jamming schemes,” Computer Communications, 160, 431-442. DOI: 10.1016/j.comcom.2020.06.026.

[2] F. A. Alzahrani, M. Ahmad, and M. T. J. Ansari, (2022). “Towards design and development of security assessment framework for Internet of medical things,” Applied Sciences, 12(16), 8148. DOI: https://doi.org/10.3390/app12168148.

[3] A. Ali, B. A. S. Al-Rimy, F. S. Alsubaei, and A. A. Almazroi, (2023). “HealthLock: Blockchain-based privacy preservation using homomorphic encryption in Internet of things healthcare applications,” Sensors, 23(15), 6762. DOI: https://doi.org/10.3390/s23156762.

[4] S. Alam, M. Shuaib, S. Ahmad, D. N. K. Jayakody, A. Muthanna, S. Bharany, and I. A. Elgendy, (2022). “Blockchain-based solutions supporting reliable healthcare for fog computing and Internet of medical things (IoMT) integration,” Sustainability, 14(22), 15312. DOI: https://doi.org/10.3390/su142215312.

[5] Z. Sheila, (2022). “Lack of well-defined responsibilities affects IoMT,” NetworkKing. Available in https://network-king.net/lack-of-well-defined-responsibilities-affects-iomt/

[6] S. A. Yousiff, R. A. Muhajjar, and M. H. Al-Zubaidie, (2023). “Designing a blockchain approach to secure firefighting stations based Internet of Things,” Informatica, 47(10). DOI: https://doi.org/10.31449/inf.v47i10.5395.

[7] M. Al-Zubaidie, Z. Zhang, and J. Zhang, (2019). “RAMHU: A new robust lightweight scheme for mutual users authentication in healthcare applications,” Security and Communication Networks, 2019. DOI: https://doi.org/10.1155/2019/3263902.

[8] M. Al-Zubaidie, and G. S. Shyaa, (2023). “Applying detection leakage on hybrid cryptography to secure transaction information in e-commerce apps,” Future Internet, 15(8), 262. DOI: https://doi.org/10.3390/fi15080262.

[9] G. S. Shyaa, and M. Al-Zubaidie, (2023). “Utilizing trusted lightweight ciphers to support electronic-commerce transaction cryptography,” Applied Sciences, 13(12), 7085. DOI: https://doi.org/10.3390/app13127085.

[10] M. Alalhareth, and S. C. Hong, (2023). “An improved mutual information feature selection technique for intrusion detection systems in the Internet of medical things,” Sensors, 23(10), 4971. DOI: https://doi.org/10.3390/s23104971.

[11] J. Su, R. Ren, Y. Li, R. Y. Lau, and Y. Shi, (2022). “Trusted blockchain-based signcryption protocol and data management for authentication and authorization in VANETs,” Wireless Communications and Mobile Computing, 2022. DOI: https://doi.org/10.1155/2022/9572992.

[12] Z. He, and H. Sayadi, (2023, April). “Image-based Zero-day malware detection in IoMT devices: A hybrid AI-enabled method,” In 2023 24th International Symposium on Quality Electronic Design (ISQED) (pp. 1-8). IEEE. DOI: https://doi.org/10.1109/ISQED57927.2023.10129348.

[13] M. S. I. Alsumaidaie, K. M. A. Alheeti, and A. Alaloosy, (2023). "Intelligent detection of distributed denial of service attacks: A supervised machine learning and ensemble approach,” Iraqi Journal for Computer Science and Mathematics Vol. 4 No. 3 (2023) p. 12-24. DOI: https://doi.org/ 10.52866/ijcsm.2023.02.03.002.

[14] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, (2024). “Insights into Internet of medical things (IoMT): Data fusion, security issues and potential solutions,” Information Fusion, 102, 102060. DOI: https://doi.org/10.1016/j.inffus.2023.102060.

[15] S. A. Salman, A. M. Sagheer, and S. Al-Janabi, (2023). “Security attacks on e-voting system using blockchain,” Iraqi Journal for Computer Science and Mathematics Vol. 4 No. 2 (2023) p. 179-188. DOI: https://doi.org/10.52866/ijcsm.2023.02.02.016.

[16] B. Shohini, R. B. Jonathan, L. Wen-Ming, F. Berta, and T. H. John, (2020). The Alice Dataset: fMRI Dataset to Study Natural Language Comprehension in the Brain. OpenNeuro. [Dataset] DOI: https://doi.org/10.18112/openneuro.ds002322.v1.0.4

[17] B. A. Sassani, M. Alkorbi, N. Jamil, M. A. Naeem, and F. Mirza, (2020). ”Evaluating encryption algorithms for sensitive data using different storage devices,” Scientific Programming, 2020, 1-9. DOI: https://doi.org/10.1155/2020/6132312.

[18] M. Mustafa, M. Alshare, D. Bhargava, R. Neware, B. Singh, and P. Ngulube, (2022). "Perceived security risk based on moderating factors for blockchain technology applications in cloud storage to achieve secure healthcare systems," Computational and mathematical methods in medicine, 2022. DOI: https://doi.org/10.1155/2022/6112815.

[19] W. U. Hassan, A. Bates, and D. Marino, (2020, May). "Tactical provenance analysis for endpoint detection and response systems," In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 1172-1189). IEEE.